

1 What is claimed is:

2

3 1. A method of generating a pseudo-random number, said method

4 comprising the steps of:

5 (a) Establish initialization values for output series of pseudo-random number

6 matrices $X_1 - X_k$;

7 (b) Establish initialization values for variable transition matrices $A_{1,1} - A_{k,1}$;

8 (c) Establish initialization values for variable offset matrices $B_{1,1} - B_{j,1}$;

9 (d) Establish first modulus operators $m_{1,1} - m_{i,1}$;

10 (e) Apply said transition matrices $A_{1,1} - A_{k,1}$ to said output series of pseudo-

11 random number matrices $X_1 - X_k$ to generate a first intermediate matrix value $X_{\text{firsttemp}}$;

12 (f) Apply said offset matrices $B_{1,1} - B_{j,1}$ to said first intermediate matrix value

13 $X_{\text{firsttemp}}$ to generate a second intermediate matrix value X_{temp} ; and

14 (g) Sequentially apply said first modulus operators $m_{1,1} - m_{i,1}$ to said second

15 intermediate matrix value X_{temp} to generate an output value of pseudo-random number

16 matrix X_n from which at least one pseudo-random number is extracted.

17

18 2. A method of generating a plurality of pseudo-random numbers, said

19 method comprising the steps of:

20 (a) Establish initialization values for output series of pseudo-random number

21 matrices $X_1 - X_k$;

22 (b) Establish initialization values for variable transition matrices $A_{1,1} - A_{k,1}$;

23 (c) Establish initialization values for variable offset matrices $B_{1,1} - B_{j,1}$;

24 (d) Establish first modulus operators $m_{1,1} - m_{i,1}$;

25 (e) Apply said transition matrices $A_{1,1} - A_{k,1}$ to said output series of pseudo-

26 random number matrices $X_1 - X_k$ to generate a first intermediate matrix value $X_{\text{firsttemp}}$;

27 (f) Apply said offset matrices $B_{1,1} - B_{j,1}$ to said first intermediate matrix value

28 $X_{\text{firsttemp}}$ to generate a second intermediate matrix value X_{temp} ;

29 (g) Sequentially apply said first modulus operators $m_{1,1} - m_{i,1}$ to said second

30 intermediate matrix value X_{temp} to generate a first output value of pseudo-random number

31 matrix X_n from which at least one pseudo-random number is extracted;

1 (h) Store said first output value matrix X_n in a storage register to establish an
2 updated output series of pseudo-random number matrices;
3 (i) Update said transition matrices $A_{1,1} - A_{k,1}$ through updating process to
4 create updated transition matrices $A_{1,2} - A_{k,2}$;
5 (j) Apply said updated transition matrices $A_{1,2} - A_{k,2}$ to said updated output
6 series of pseudo-random number matrices $X_{n-k+1} - X_n$ to generate an updated first
7 intermediate matrix value $X_{\text{firsttemp}}$;
8 (k) Update said offset matrices $B_{1,1} - B_{j,1}$ through updating process to create
9 updated offset matrices $B_{1,2} - B_{j,2}$;
10 (l) Apply said updated offset matrices $B_{1,2} - B_{j,2}$ to said updated first
11 intermediate matrix value $X_{\text{firsttemp}}$ to generate an updated second intermediate matrix
12 value X_{temp} ;
13 (m) Update said first modulus operators $m_{1,1} - m_{i,1}$ through updating process to
14 create updated first modulus operators $m_{1,2} - m_{i,2}$;
15 (n) Sequentially apply said updated first modulus operators $m_{1,2} - m_{i,2}$ to said
16 updated second intermediate matrix value X_{temp} to generate a second output value of
17 pseudo-random number matrix X_{n+1} from which at least one pseudo-random number is
18 extracted; and
19 (o) Store said second pseudo-random number matrix X_{n+1} in said storage
20 register of pseudo-random number matrices.
21
22 3. A method of generating a plurality of pseudo-random numbers according
23 to claim 2, wherein said steps i. through o. are repeated to generate a desired number d of
24 pseudo-random number matrices X_{n+d} from which a plurality of pseudo-random numbers
25 are extracted.
26
27 4. A method according to claim 2 further comprising the step of:
28 Selecting a first subset of said pseudo-random numbers from said updated
29 output series of pseudo-random number matrices .
30

- 1 5. A method according to claim 1, claim 2, or claim 3, wherein $k = 1$ so that
2 a single variable transition matrix is used.
3
- 4 6. A method according to claim 1, claim 2, or claim 3, where $j = 1$ so that a
5 single variable offset matrix is used.
6
- 7 7. A method according to claim 1, claim 2, or claim 3, where $i = 1$ so that a
8 single modulus operator is used.
9
- 10 8. A method according to claim 2, further comprising the steps of:
11 (a) Establish second modulus operators $r_{1,1} - r_{g,1}$;
12 (b) Sequentially apply and update second modulus operators $r_{1,1} - r_{g,1}, r_{1,2} -$
13 $r_{g,2}, \dots r_{1,n+d-k} - r_{g,n+d-k}$ to said updated output series of pseudo-random number matrices to
14 generate a second output series of pseudo-random number matrices.
15
- 16 9. A method according to claim 8, further comprising the step of:
17 Selecting a second subset of said pseudo-random numbers from said
18 second output series of pseudo-random number matrices.
19
- 20 10. A method according to claim 1, claim 2, or claim 3:
21 (a) Wherein said first modulus operators $m_{1,1} - m_{j,1}, m_{1,2} - m_{j,2}, \dots m_{1,n+d-k} -$
22 $m_{j,n+d-k}$ comprise a uniform variable modular reduction, and
23 (b) Further comprising the step of discarding certain pseudo-random numbers
24 which are not uniformly distributed.
25
- 26 11. A method according to claim 8:
27 (a) Wherein said second modulus operators $r_{1,1} - r_{g,1}, r_{1,2} - r_{g,2}, \dots r_{1,n+d-k} -$
28 $r_{g,n+d-k}$ comprise a uniform variable modular reduction, and
29 (b) Further comprising the step of discarding certain pseudo-random numbers
30 which are not uniformly distributed.
31

- 1 12. A method according to claim 2 or claim 3, further comprising the steps of:
- 2 (a) Create at least one other storage register of pseudo-random number
- 3 matrices by separately taking steps a – o;
- 4 (b) Create temporary composite pseudo-random number matrices by combining
- 5 each resulting storage register of pseudo-random number matrices through at least one
- 6 mathematical operation;
- 7 (c) Create final composite pseudo-random number matrices by applying
- 8 variable modular reduction to said temporary composite pseudo-random number
- 9 matrices; and
- 10 (d) Select a subset of pseudo-random numbers from said resulting final
- 11 composite pseudo-random number matrices
- 12
- 13 13. A method according to claim 1, claim 2, or claim 3 further comprising:
- 14 (a) Apply an invertibility evaluation module to each second intermediate
- 15 matrix value X_{temp} ;
- 16 (b) Adjust offset matrices $B_{1,1} - B_{j,1}, B_{1,2} - B_{j,2}, \dots B_{1,n+d-1} - B_{j,n+d-1}$, so that
- 17 said second intermediate matrix value X_{temp} is non-invertible;
- 18 (c) Sequentially apply said first modulus operators $m_{1,1} - m_{i,1}$ to said non-
- 19 invertible second intermediate matrix value X_{temp} to generate output value of non-
- 20 invertible pseudo-random number matrix X_n from which at least one pseudo-random
- 21 number is extracted; and
- 22 (d) Select a subset of pseudo-random number output values from said non-
- 23 invertible pseudo-random number matrices
- 24
- 25 14. An apparatus for generating a pseudo-random number, said apparatus
- 26 comprising:
- 27 (a) Output matrices initialization means for establishing initialization values
- 28 for output series of pseudo-random number matrices $X_1 - X_k$;
- 29 (b) Transition matrices initialization means for establishing initialization
- 30 values for variable transition matrices $A_{1,1} - A_{k,1}$;

1 (c) Offset matrices initialization means for establishing initialization values
2 for variable offset matrices $B_{1,1} - B_{j,1}$;

3 (d) Modulus operator means for establishing first modulus operators $m_{1,1} -$
4 $m_{i,1}$;

5 (e) First application means for applying said transition matrices $A_{1,1} - A_{k,1}$ to
6 said output series of pseudo-random number matrices $X_1 - X_k$ to generate a first
7 intermediate matrix value $X_{firsttemp}$;

8 (f) Second application means for applying said offset matrices $B_{1,1} - B_{j,1}$ to
9 said first intermediate matrix value $X_{firsttemp}$ to generate a second intermediate matrix
10 value X_{temp} ; and

11 (g) Third application means for sequentially applying said first modulus
12 operators $m_{1,1} - m_{i,1}$ to said second intermediate matrix value X_{temp} to generate an output
13 value of pseudo-random number matrix X_n from which at least one pseudo-random
14 number is extracted.

15

16 15. An apparatus for generating a plurality of pseudo-random
17 numbers, said apparatus comprising:

18 (a) Output matrices initialization means for establishing initialization values
19 for output series of pseudo-random number matrices $X_1 - X_k$;

20 (b) Transition matrices initialization means for establishing initialization
21 values for variable transition matrices $A_{1,1} - A_{k,1}$;

22 (c) Offset matrices initialization means for establishing initialization values
23 for variable offset matrices $B_{1,1} - B_{j,1}$;

24 (d) Modulus operator means for establishing first modulus operators $m_{1,1} -$
25 $m_{i,1}$;

26 (f) First application means for applying said transition matrices $A_{1,1} - A_{k,1}$ to
27 said output series of pseudo-random number matrices $X_1 - X_k$ to generate a first
28 intermediate matrix value $X_{firsttemp}$;

29 (g) Second application means for applying said offset matrices $B_{1,1} - B_{j,1}$ to
30 said first intermediate matrix value $X_{firsttemp}$ to generate a second intermediate matrix
31 value X_{temp} ;

1 (h) Third application means for sequentially applying said first modulus
2 operators $m_{1,1} - m_{i,1}$ to said second intermediate matrix value X_{temp} to generate a first
3 output value of pseudo-random number matrix X_n from which at least one pseudo-
4 random number is extracted;

5 (i) Storage means for storing said first output value matrix X_n in a storage
6 register to establish an updated output series of pseudo-random number matrices;

7 (j) Transition matrices updating means for updating said transition matrices
8 $A_{1,1} - A_{k,1}$ to create updated transition matrices $A_{1,2} - A_{k,2}$;

9 (k) Fourth application means for applying said updated transition matrices
10 $A_{1,2} - A_{k,2}$ to said updated output series of pseudo-random number matrices $X_{n-k+1} - X_n$ to
11 generate an updated first intermediate matrix value $X_{firsttemp}$;

12 (l) Offset matrices updating means for updating said offset matrices $B_{1,1} - B_{j,1}$
13 to create updated offset matrices $B_{1,2} - B_{j,2}$;

14 (m) Fifth application means for applying said updated offset matrices $B_{1,2} -$
15 $B_{j,2}$ to said updated first intermediate matrix value $X_{firsttemp}$ to generate an updated second
16 intermediate matrix value X_{temp} ;

17 (n) Modulus operator updating means for updating said first modulus
18 operators $m_{1,1} - m_{i,1}$ to create updated first modulus operators $m_{1,2} - m_{i,2}$;

19 (o) Sixth application means for sequentially applying said updated first
20 modulus operators $m_{1,2} - m_{i,2}$ to said updated second intermediate matrix value X_{temp} to
21 generate a second output value of pseudo-random number matrix X_{n+1} from which at
22 least one pseudo-random number is extracted; and

23 (p) Second storage means for storing said second pseudo-random number
24 matrix X_{n+1} in said storage register of pseudo-random number matrices.

25
26
27
28
29
30
31